

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

In re Application of the United	§	Magistrate No. H-10-998M
States of America for Historical	§	Magistrate No. H-10-990M
Cell Site Data	§	Magistrate No. H-10-981M

Government's Memorandum Of Law In Support Of Request For Review

The United States of America, by and through its United States Attorney, José Angel Moreno, and Eric D. Smith, Assistant United States Attorney for the Southern District of Texas, and Nathan Judish, Senior Counsel, Computer Crime and Intellectual Property Section, United States Department of Justice, hereby seeks review of the Opinion entered on October 29, 2010, by United States Magistrate Judge Stephen Smith in matters Magistrate Nos. H-10-998M, H-10-990M, and H-10-981M (hereinafter, the "Opinion") (attached as Exhibit A). The Opinion denied three applications by the United States seeking disclosure of historical cell-site records pursuant to § 2703(c) and (d) of the Stored Communications Act ("SCA"), 18 U.S.C. § 2703(c) & (d).¹ For the reasons set forth below, the government respectfully submits that this Court should reverse the Opinion and grant the applications for historical cell-site information.

Procedural History

On October 5, 2010, the United States submitted an application and proposed order for an order under 18 U.S.C. § 2703(d) (a "2703(d) order") to compel T-Mobile to disclose, among various classes of information, "historical cellsite information and call detail records (including

¹ The Opinion has been submitted for publication. *See In re Application of the United States for Historical Cell Site Data*, ___ F. Supp. 2d ___, 2010 WL 4286365 (S.D. Tex. Oct. 29, 2010).

in two-way radio feature mode) for the sixty (60) days prior to the date this Order is signed by the Court.” October 5 Application at 2. The application defined cell-site information to include “the antenna tower and sector to which the cell phone sends its signal.” *Id.* at 2 n.5² On October 6 and October 12, 2010, the United States submitted similar applications for orders directed to MetroPCS and T-Mobile. *See* October 6 and October 12 Applications. As required by § 2703(d), each of these applications set forth specific and articulable facts showing that there are reasonable grounds to believe that the historical cell-site records sought were relevant and material to an ongoing criminal investigation.

On October 14, 2010, Magistrate Judge Smith issued an order directing the United States to file a brief addressing its applications for historical cell-site records. The court also noted its intent to take judicial notice from certain categories of facts, including “(1) congressional testimony at recent hearings before House and Senate committees on ECPA reform; (2) published surveys and studies by telecommunications industry groups such as CTIA regarding cell sites and cell phone usage; (3) published reports and product specifications concerning current microcell technology; and (4) published privacy policies of providers regarding call location information.” October 14 Order at 1-2. The court invited the government to make objections or proposed additions “to these categories of judicially noticed facts.” *Id.* at 2. However, the court failed to give notice to the United States of any particular facts of which it intended to take judicial notice. In its brief filed on October 25, 2010, the United States

²The application defined “call detail records” to include “the cellsite/sector(s) used by the mobile telephone to obtain service for a call or when in an idle state.” Upon further inquiry, counsel for the United States now believes that cell phone service providers do not create cell-site records when a phone is in an idle state. Thus, the United States is willing to exclude such information from the scope of its application.

responded that it “cannot determine from the broad categories cited by the Court whether it is appropriate to take judicial notice of any particular facts that might fall within those categories.” Government’s Memorandum of Law at 23. The United States further stated that “it is appropriate to take judicial notice of providers’ terms of service and privacy policies for the purpose of establishing the contractual relationship between customers and providers,” but it objected to taking judicial notice of congressional testimony, as well as published surveys, studies, or reports by industry groups. *Id.*

On October 29, 2010, Magistrate Judge Smith issued an opinion denying the United States’s applications and declaring that “warrantless disclosure of cell site data violates the Fourth Amendment.” Opinion at 35. The opinion began with fifty paragraphs of “findings of fact” that address the structure of phone companies’ cellular networks, the location information generated by the phone companies, the accuracy of the location information generated by the phone companies, and the kind of location information stored and retained by service providers. The “findings of fact” never mention T-Mobile or MetroPCS specifically; in fact, only one paragraph of the “findings of fact” mentions any specific cell phone providers. *See* Opinion at ¶ 24. The findings include claims that “a provider can pinpoint the phone’s latitude and longitude to an accuracy within 50 meters or less,” that carriers create records “that include the most accurate location information available to them,” and that historical cell-site data “is sufficient to plot the target’s movements hour by hour for the duration of the 60 day period covered by the government’s request.” Opinion at ¶¶ 27, 31, 49.

The court asserted that these findings were “appropriate for judicial notice under Rule 201 of the Federal Rules of Evidence.” Opinion at 5. The court’s findings regarding provider

networks and record keeping were largely based on statements made before Congress by Matt Blaze, an Associate Professor of Computer and Information Science at the University of Pennsylvania. *See* Opinion at 5-13 (citing Blaze’s testimony in footnotes 13-17, 19, 21-35, 37-40, 42-46, and 51-55). According to the Opinion, taking judicial notice of Blaze’s congressional testimony was proper because it was “not offered for partisan purposes or to advocate specific legislation.” Opinion at 5.

The Opinion then addressed the compelled disclosure of historical cell-site records by analyzing them under legal standards courts have used for information gained from tracking devices surreptitiously installed by the government. The Opinion held that “compelled warrantless disclosure of cell site data violates the Fourth Amendment under the separate authorities of [*United States v. Karo*, 468 U.S. 705 (1984)] and [*United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010)].” Opinion at 35. It rejected application of the Supreme Court’s cases concerning compelled disclosure of business records, asserting that cell-site information was not “voluntarily conveyed” to a provider and that “[i]f the telephone numbers dialed in *Smith v. Maryland* were notes on a musical scale, the location data sought here is a grand opera.” Opinion at 33-34. The Opinion also cited and joined a recent magistrate decision from the Eastern District of New York which relied heavily on *Maynard* in holding that a warrant was required to compel disclosure of historical cell site information. *See* Opinion at 3, 20, 22-24 (citing *In re Application of United States*, ___ F. Supp. 2d ___, 2010 WL 3463132 (E.D.N.Y. Aug. 27, 2010)). On November 29, 2010, that magistrate decision was reversed by the reviewing district court, with an opinion to follow. *See In re Application of United States*, No. 10-0550, (E.D.N.Y. Nov. 29, 2010) (unpublished order).

On November 12, 2010, Magistrate Judge Smith granted the United States's motion to extend the deadline for filing its objections to the Opinion until December 3, 2010.

Argument

The United States objects to both the Opinion's improper use of judicial notice and its Fourth Amendment analysis and conclusions. Regarding the "findings of fact," the United States objects to Magistrate Judge Smith's failure to provide the United States with appropriate prior notice and to taking judicial notice of facts subject to reasonable dispute. Moreover, based on a sworn affidavit from MetroPCS and discussions with T-Mobile, the United States believes that Magistrate Judge Smith's "findings of fact" are inaccurate or misleading.³ This Court should reject Magistrate Judge's Smith's "findings of fact" because they are "subject to reasonable dispute" under Rule 201 of the Federal Rules of Evidence.

Regarding the Fourth Amendment, there are three separate and independent reasons why the United States's use of a 2703(d) order to compel disclosure of historical cell-site records is consistent with the Fourth Amendment. First, a customer has no privacy interest in business records held by a cell phone provider, as they are not the customer's private papers. Second, this case involves compulsory process, and the Fourth Amendment sets a reasonableness standard rather than a warrant requirement for compulsory process. Third, even under the standards applicable to surreptitiously installed tracking devices, the Fourth Amendment would not bar compelled disclosure of historical cell-site records, because such records do not establish a phone's location with sufficient precision to place the phone in a location protected by a

³T-Mobile's representatives expressed a preference for direct communication with the court regarding their historical cell-site records and declined to submit an affidavit.

reasonable expectation of privacy.

Significantly, neither of the first two Fourth Amendment objections requires this Court to make factual findings regarding the historical cell-site information stored by service providers in order to reverse the Opinion. However, if this Court wishes to make findings of fact regarding the precision of T-Mobile's historical cell-site records, it may be helpful for this Court to obtain testimony from T-Mobile on that topic. Such a hearing is not essential to this case: the United States submits that this Court should reverse the Opinion because a customer has no privacy interest in business records held by a cell phone provider and because the Fourth Amendment sets a reasonableness standard for compulsory process.

I. Judicial Notice

A. The Court Failed to Provide Appropriate Prior Notice of Judicially-Noticed Facts.

Under Rule 201(e), “[a] party is entitled upon timely request to an opportunity to be heard as to the propriety of taking judicial notice and the tenor of the matter noticed.” As the Advisory Committee Note to Subdivision (e) explains, “[b]asic considerations of procedural fairness demand an opportunity to be heard on the propriety of taking judicial notice.” *See also United States v. Garcia*, 672 F.2d 1349, 1356 n. 9 (11th Cir. 1982) (“Ordinarily, when a judge takes judicial notice of a fact other than at the request of a party (i.e., ‘discretionary judicial notice’), he should notify the parties that he is doing so and afford them an opportunity to be heard.”). Moreover, a party has a due process right to notice when a court takes judicial notice. *See* 21B Wright and Graham, *Federal Practice and Procedure* § 5107 (2d ed. 2005) (discussing constitutional requirements of notice).

Prior to issuing the Opinion, Magistrate Judge Smith did not inform the United States of

the specific facts of which he intended to take judicial notice. Instead, the court only informed the United States of the broad categories from which he intended to draw facts. *See* October 14 Order at 1-2. The United States objected that it could not “determine from the broad categories cited by the Court whether it is appropriate to take judicial notice of any particular facts that might fall within those categories.” Government’s Memorandum of Law at 23. By providing the United States with notice only of broad categories, rather than specific facts, Magistrate Judge Smith did not provide the United States with a reasonable opportunity to respond to the judicially-noticed facts. The court’s failure to give notice of the specific facts of which it intended to take judicial notice violated Rule 201 of the Federal Rules of Evidence.

B. The Court Improperly Took Judicial Notice of Facts Subject to Reasonable Dispute.

Magistrate Judge Smith erred in taking judicial notice of congressional testimony about the structure of the phone companies’ cellular networks, the location information generated by the phone companies, the accuracy of the location information generated by the phone companies, and the kind of location information stored and retained by service providers. Under Rule 201 of the Federal Rules of Evidence, “[a] judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned.” As the Advisory Committee Notes to Rule 201 caution, “[a] high degree of indisputability is the essential prerequisite.” Advisory Committee Note to Subdivision (a). Indeed, “the tradition has been one of caution in requiring that the matter be beyond reasonable controversy.” *Id.* at Note to Subdivision (b).

The Fifth Circuit has repeatedly confirmed these stringent requirements for judicial

notice: “judicial notice applies to self-evident truths that no reasonable person could question, truisms that approach platitudes or banalities.” *Hardy v. Johns-Manville Sales Corp.*, 681 F.2d 334, 347 (5th Cir. 1982). In *Hardy*, the Fifth Circuit held that the district court erred in taking judicial notice of the proposition that asbestos causes cancer. The court explained that “[t]he proposition that asbestos causes cancer, because it is inextricably linked to a host of disputed issues . . . is not at present so self-evident a proposition as to be subject to judicial notice.” The court concluded that “[t]he rule of judicial notice ‘contemplates there is to be no evidence before the jury in disproof.’ . . . Surely where there is evidence on both sides of an issue the matter is subject to reasonable dispute.” *Id.* at 348. *See also Taylor v. Charter Medical Corp.*, 162 F.3d 827, 830 (5th Cir. 1998) (proposition that a particular hospital was a state actor “was not the type of self-evident truth that no reasonable person could question, a truism that approaches platitude or banality, as required to be eligible for judicial notice under Rule 201” (internal quotation marks and brackets omitted)).

Of the fifty paragraphs of the Opinion’s Rule 201 “findings of fact,” only the first paragraph, which states that cellular phones use radio waves to communicate with the telephone network, is appropriate for judicial notice under Rule 201. The Opinion relies primarily on congressional testimony of Matt Blaze, an Associate Professor of Computer and Information Science at the University of Pennsylvania. *See* Opinion at 5-13 (citing Blaze’s testimony in footnotes 13-17, 19, 21-35, 37-40, 42-46, and 51-55). This testimony, which addresses both the structure of provider networks and their internal record keeping practices, addresses matters far from platitudes, banalities, or self-evident truths. As discussed in section I.C below, the “findings of fact” are contradicted by the sworn affidavit of MetroPCS, and based on discussions

with representatives of T-Mobile, the United States believes the “findings of fact” do not accurately describe T-Mobile’s historical cell-site records either. The “findings of fact” are also inconsistent with other court decisions and findings of the FCC. *See, e.g., In re Applications of United States*, 509 F. Supp. 2d 76, 78 n.3 (D. Mass. 2007) (“In urban areas, cell towers can be only hundreds of feet apart. In rural areas, towers are often ten miles or more apart.”); *In re Revision of the Commission’s Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, 15 FCC Rcd. 17442, 17462 (Sept. 8, 2000) (finding that a certain location-finding technique accurate to within 500-1000 meters “would be significantly more precise” than “the location of the cell site or sector receiving the call.”). Given the differences between Professor Blaze’s testimony and the findings of other courts, the FCC, and the sworn affidavit from MetroPCS, the “findings of fact” are subject to reasonable dispute and therefore not an appropriate subject for judicial notice.

On June 24, 2010, Magistrate Judge Smith and Professor Blaze testified on the same panel before a congressional committee regarding the Electronic Communications Privacy Act . *See ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 12-31, 76-94 (2010). Essentially, Magistrate Judge Smith has now chosen to adopt Professor Blaze’s out-of-court testimony as indisputable fact. This is improper. The Opinion offers no caselaw support for its extensive use of judicial notice and instead asserts that taking judicial notice of Professor Blaze’s congressional testimony was proper because it was “not offered for partisan purposes or to advocate specific legislation.” Opinion at 5. This characterization may reflect a somewhat overly optimistic view of the legislative process, but

even if true, nonpartisan statements that do not advocate specific legislation remain subject to reasonable dispute under Rule 201. Adopting Professor Blaze's testimony as indisputable fact violates the principle that "[j]udicial notice is denied to disputable propositions found in testimony at government hearings." 1 Jack B. Weinstein & Margaret A. Berger, *Weinstein's Federal Evidence* § 201.13[1][c] (McLaughlin ed., 2d ed. 2010).

C. The Court's Factual Findings are Misleading or Inaccurate.

The United States's objections to Magistrate Judge Smith's "findings of facts" are not merely procedural: the United States believes that critical portions of the "findings of fact" are vague, misleading, or incorrect. Magistrate Judge Smith's Opinion states that the court has been mindful of the "admonition to base a Fourth Amendment adjudication on an adequate factual record," Opinion at 4, a record that is vague or incorrect is not adequate.

MetroPCS has now submitted a sworn affidavit regarding its historical cell-site records. *See* Exhibit B. This affidavit indicates that the average MetroPCS "towers have a coverage radius of about one to two miles," and the radius is "no smaller than 100 yards in some densely populated urban areas." Exhibit B ¶ 4. In addition, "MetroPCS does not create and store cell-site information unless a call is made;" it stores only a record of a single tower the phone was connected to at the beginning and end of the call; and it does not store cell-site records when a phone is idle. Exhibit B ¶¶ 7, 8, 9. From the United States's conversations with representatives of T-Mobile, the United States believes that T-Mobile would provide to this Court similar information regarding historical cell-site information produced by T-Mobile.

These statements of MetroPCS and T-Mobile directly conflict with the assertions in the "findings of fact" that "a provider can pinpoint the phone's latitude and longitude to an accuracy

within 50 meters or less,” that carriers create records “that include the most accurate location information available to them,” that “[s]ome carriers also store frequently updated, highly precise, location information not just when calls are made or received, but as the device moves around the network,” and that “[t]his data is sufficient to plot the target’s movements hour by hour for the duration of the 60 day period covered by the government’s request.” Opinion at ¶¶ 27, 31, 33, and 49. Similarly, the “findings of fact” assert that “call detail records can now include the user’s latitude and longitude.” Opinion at ¶ 33. But MetroPCS does not store latitude/longitude information, Exhibit B ¶ 10, and the United States believes (based on statements from T-Mobile’s representatives) that T-Mobile does not store historical latitude/longitude information either.

Thus, on the core issues regarding the accuracy of historical cell-site records, the United States believes the judicially noticed “findings of fact” are incorrect. Because all of the “findings of fact” (other than ¶1) are not appropriate for judicial notice under Rule 201, the United States will only briefly address objections to other individual “findings of fact.” Some “findings of fact,” including paragraphs 17, 18, 25, 26, 34, and 42 are vague. For example, paragraph 17’s assertion that “the size of the typical cell sector has been steadily shrinking” is vague, as it tells us nothing about the size of cells or the rate at which they are allegedly shrinking. No “findings of fact” specifically reference T-Mobile and MetroPCS, the two providers at issue in this case, and the “findings of fact” frequently contain generalizations about “some,” “many,” or “most” providers without specifying which providers engage in the practices alleged. *See* Opinion ¶¶ 29, 33, 35, 39. Other “findings of fact,” including paragraphs 41, 50, and portions of 42 and 49 are not even facts: they are opinions, hypothetical speculation, inferences, or predictions about the

future. *See* 21B Wright and Graham, *Federal Practice and Procedure* § 5104 (“opinion-facts,” including inferences and statements about the future, are not generally appropriate for judicial notice). The United States also specifically questions the accuracy of other “findings of fact,” including paragraphs 4, 5, 18, 24, and 33. For example, paragraph 5 asserts that a handoff between cell towers will occur during a call “if the phone moves nearer to another base station,” but the United States believes that this does not necessarily happen, and that the handoff process is more complex than this paragraph suggests. In any case, a court cannot take judicial notice of such facts under Rule 201, because they are subject to reasonable dispute.

II. The Fourth Amendment

Historical cell-site records are business records generated and stored by cell phone companies when their customers make or receive telephone calls. Indeed, even Magistrate Judge Smith concedes that historical cell-site records are “generated in the ordinary course of the provider’s business.” Opinion at 26. The Opinion nevertheless concludes that the Fourth Amendment requires a warrant to compel disclosure of historical cell-site information based on analogy to cases involving tracking devices surreptitiously installed by the government. *See* Opinion at 35 (holding that “compelled warrantless disclosure of cell site data violates the Fourth Amendment under the separate authorities of *Karo* and *Maynard*”). As explained below, this is incorrect for three reasons, the first two of which do not require this Court to make factual findings regarding the precision of historical cell-site information. First, a customer has no privacy interest in business records held by a cell phone provider, as they are not the customer’s private papers. Second, this case involves compulsory process, not a surreptitiously installed tracking device, and the Fourth Amendment sets a reasonableness standard for compulsory

process, not a warrant requirement. Third, even under the standards applicable to surreptitiously installed tracking devices, the Fourth Amendment does not bar compelled disclosure of historical cell-site records. The United States submits that this Court should reverse the Opinion because a customer has no privacy interest in business records held by a cell phone provider and because the Fourth Amendment sets a reasonableness standard for compulsory process.

A. A customer has no privacy interest in a cell phone provider's historical cell-site records.

A cell phone customer has no Fourth Amendment privacy interest in historical cell-site records because such records are business records held by a third party, not the customer's private papers. Addressing a Fourth Amendment challenge to a third party subpoena for bank records, the Supreme Court held in *United States v. Miller*, 425 U.S. 435 (1976), that the bank's records "are not respondent's 'private papers'" but are "the business records of the banks" in which a customer "can assert neither ownership nor possession." *Miller*, 425 U.S. at 440. The records "pertain to transactions to which the bank was itself a party." *Id.* at 441. As the United States Court of Appeals for the District of Columbia Circuit stated, "it has been consistently held by the Supreme Court and the Courts of Appeals that a person has no Fourth Amendment basis for challenging subpoenas directed at the business records of a third party." *Reporters Committee for Freedom of Press v. AT&T*, 593 F.2d 1030, 1044 (D.C. Cir. 1978) (citing cases).

Historical cell-site records are business records kept by the cell phone company of the cell towers it used to process a particular call. See *United States v. Garcia-Alvarez*, 2007 WL 996162 at *1 (D.P.R. 2007) ("The location of the cell site for each call appears as a billing code in each customer's cell phone records."). Thus, a customer has no Fourth Amendment interest in

historical cell-site records. Like the bank records in *Miller*, a customer has neither ownership, possession, or control over historical cell-site records stored by a provider. The choice to create and store historical cell-site records is made by the provider, not the customer, and the provider controls the format, content, and duration of the records it chooses to create and retain. Indeed, because cell-site records are not in the possession of a customer, a customer could not be expected to produce cell-site records in response to a subpoena for his own cell-site records. Moreover, although a customer is likely to be aware that the cell phone company will assign a cell tower to handle his call, the customer typically does not know which cell tower is assigned to process his calls. Thus, cell-site records cannot be a customer's "private papers." Similarly, the assignment of a particular cell tower to process a call is a transaction to which the cell phone company is a party: the assignment is made by the cell phone company to facilitate the functioning of its network. Therefore, a customer's historical cell-site records are not protected by the Fourth Amendment because they are the phone company's business record rather than a customer's private papers. *See also SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) ("when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities").

The Court's reasoning in *Smith v. Maryland*, 442 U.S. 735 (1979), leads to the same result. In *Smith*, the Court held both that telephone users had no subjective expectation of privacy in dialed telephone numbers and also that any such expectation is not one that society is prepared to recognize as reasonable. *See Smith*, 442 U.S. at 742-44. The Court's reasoning applies equally to cell-site records. First, the Court stated: "we doubt that people in general

entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.” *Id.* at 742. Similarly, cell phone users understand that they must send a radio signal which is received by a cell phone company's antenna if the company is going to route their call to its intended recipient.

Second, under the reasoning of *Smith*, any subjective expectation of privacy in cell-site records is unreasonable. In *Smith*, the Court explicitly held that “even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable.” *Id.* at 743 (internal quotation omitted). It noted that “[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Id.* at 743-44. In *Smith*, the user “voluntarily conveyed numerical information to the telephone company” and thereby “assumed the risk that the company would reveal to police the numbers he dialed.” *Id.* at 744. Here, a cell phone user voluntarily transmits a signal to a cell tower for his call to be connected, and the provider thereby creates records, for its own business purposes, regarding which of its cell towers it used to complete the call. The user assumes the risk that the cell phone provider will reveal the cell-site records to law enforcement. Thus, it makes no difference if some users have never thought about how their cell phones work; a cell phone user can have no reasonable expectation of privacy in cell-site records. If anything, the privacy interest in cell-site information is even less than the privacy interest in a dialed phone number or bank records. The location of the cell phone tower handling a customer's call is generated internally by the phone company and is not typically known by the customer. A customer's

Fourth Amendment rights are not violated when the phone company reveals to the government its own records that were never in the possession of the customer.

Several recent cases have relied on *Smith* and *Miller* and rejected Fourth Amendment challenges to acquisition of historical cell-site records without a warrant. *See, e.g., United States v. Velasquez*, 2010 WL 4286276, at *5 (N.D. Cal. Oct. 22, 2010) (denying suppression of historical cell-site data); *United States v. Benford*, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010); *United States v. Suarez-Blanca*, 2008 WL 4200156, at *8-*11 (N.D. Ga. Mar. 26, 2008) (same); *Mitchell v. State*, 25 So.3d 632, 635 (Fla. Dist. Ct. App. 2009) (same). *But see In re Application of United States*, 620 F.3d 304, 313, 317 (3d Cir. 2010) (rejecting analogy to *Smith v. Maryland* for historical cell-site records, but nevertheless stating that historical cell-site records are “obtainable under a § 2703(d) order and that such an order does not require the traditional probable cause determination”). The Opinion cites one recent decision by a magistrate judge in the Eastern District of New York holding that a warrant is required to compel disclosure of historical cell-site information, but that decision has now been reversed by the district court. *See In re Application of United States*, ___ F. Supp. 2d ___, 2010 WL 3463132 (E.D.N.Y. Aug. 27, 2010), *rev’d* No. 10-0550, (E.D.N.Y. Nov. 29, 2010) (unpublished order noting opinion to follow).

Magistrate Judge Smith’s Opinion asserts that *Miller* and *Smith* are not applicable to historical cell-site information because a customer has not “voluntarily conveyed” cell-site information to the service provider. *See* Opinion at 33. This assertion is mistaken or irrelevant for two reasons, as explained below. First, cell-site information is voluntarily conveyed to the phone company under the reasoning of *Smith*. Second, voluntariness is not essential to *Miller*’s

holding that a customer has no privacy interest in a third party's business records.

Under the reasoning of *Smith*, cell-site information is voluntarily conveyed to the phone company. In *Smith*, the Supreme Court assumed that telephone users were familiar with telephone technology. *See Smith*, 442 U.S. at 742 (“All telephone users realize that they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.”). In contrast, Magistrate Judge Smith’s Opinion assumes that cell phone users are ignorant of cell phone technology (even though the Opinion assumes that cell phone technology is sufficiently indisputable to be a proper subject for judicial notice). *See Opinion* at 31. This “assumption of ignorance” is inconsistent with the Supreme Court’s reasoning in *Smith*. Moreover, users will know from their experience with cell phones that they communicate with a provider’s cell tower and that this communication will convey information to the provider about their location. Indeed, cell phone users routinely experience the frustration associated with dropped calls and recognize they are caused when their phone’s radio signal is having difficulty reaching a tower clearly. Cell phones also often display a cell tower icon, along with bars representing the strength of the signal between the phone and tower. Cell phone users also understand that the provider will know the location of its own cell tower, and that the provider will thus have some knowledge of the user’s location.

In addition, providers’ terms of service and privacy policies make clear that the providers obtain cell phone location information. For example, T-Mobile’s privacy policy includes the following provisions:

Our network detects your device's approximate location whenever it is turned on (subject to coverage limitations). This location technology makes the routing of wireless communications possible and is also the basis for providing enhanced emergency 9-1-1 service, which permits us to provide your general location to a public safety answering point, emergency medical service provider, or emergency dispatch provider.

We automatically collect certain information, some of which may be associated with personal information, whenever you use our services or Web sites. For example, our systems capture details about the type and location of wireless device(s) you use, calls and text messages you send and receive, and other data services you use (for example your ringtone purchases).

We use personal information for a variety of business purposes, including for example, to complete transactions and bill for products and services; verify your identity; respond to your requests for service or assistance; anticipate and resolve actual and potential problems with our products and services; create and improve products and services; suggest additional or different products or services; make internal business decisions about current and future offers; provide personalized service and user experiences; and protect our rights and property.

www.t-mobile.com/company/website/privacypolicy.aspx (visited December 1, 2010). The first of these paragraphs demonstrates that a cell phone customer will be aware that T-Mobile obtains information regarding the customer's location. The second paragraph demonstrates that a customer will be aware that T-Mobile collects this information. The third paragraph demonstrates that the customer will be aware that this information becomes a T-Mobile business record. Thus, under the principles of *Smith v. Maryland*, a customer voluntarily conveys location information to the cell phone company and cannot object when the cell phone company conveys that information to the government.

In addition, voluntariness is not essential to the general rule that a customer has no reasonable expectation of privacy in a third party's business records. Although *Miller* does note that the bank statements "contain only information voluntarily conveyed to the banks," *Miller*,

425 U.S. at 442, this statement comes two pages after the core paragraph of the decision, in which the Court reasons that “the documents subpoenaed here are not respondent’s ‘private papers’” but are instead “the business records of the banks,” over which a customer “can assert neither ownership nor possession.” *Miller*, 425 U.S. at 440. *See Wilson v. First Gibraltar Bank*, 1994 WL 199108, at *3 (5th Cir. May 12, 1994) (noting that the bank records of *Miller* were not protected by the Fourth Amendment because they were the “bank’s business records rather than depositor’s private papers”); *cf. United States v. Gallo*, 123 F.2d 229, 231 (2d Cir. 1941) (L. Hand, Swan, A. Hand, JJ.) (“When a person takes up a telephone he knows that the company will make, or may make, some kind of a record of the event, and he must be deemed to consent to whatever record the business convenience of the company requires.”). This rule for third-party business records is consistent with the more general Fourth Amendment principle that a person lacks a Fourth Amendment interest in an item in which he has “neither a property nor a possessory interest.” *Rakas v. Illinois*, 439 U.S. 128, 148 (1978) (holding that defendants lacked legitimate expectation of privacy in another’s automobile and others’ items in automobile). Thus, because historical cell-site records are business records of the provider, the government may use a 2703(d) order to compel their disclosure.

The Opinion also errs in suggesting that a separate statute, the Wireless Communication and Public Safety Act of 1999 (“WCPSA”), is relevant to whether there is an expectation of privacy under the Fourth Amendment in historical cell-site information. *See* Opinion at 26-29. Any argument that the WCPSA creates a Fourth Amendment privacy interest has now been foreclosed by the Supreme Court’s recent rejection of the proposition that statutes can create a constitutional reasonable expectation of privacy. In *City of Ontario v. Quon*, 130 S. Ct. 2619

(2010), Quon argued that a violation of § 2702 of the SCA rendered a search of his text messages unreasonable under the Fourth Amendment. The Supreme Court rejected the notion that the SCA created Fourth Amendment rights: “Respondents point to no authority for the proposition that the existence of statutory protection renders a search per se unreasonable under the Fourth Amendment. And the precedents counsel otherwise.” *Id.* at 2632 (citing *Virginia v. Moore*, 553 U.S. 164, 168 (2008) and *California v. Greenwood*, 486 U.S. 35, 43 (1988)).

In any case, the WCPSA allows compelled disclosure pursuant to the SCA. In particular, the WCPSA amended 18 U.S.C. § 222, which provides that “[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information” in certain specified situations. 47 U.S.C. § 222(c)(1) (emphasis added). The phrase “except as required by law” encompasses appropriate criminal legal process. *See Parastino v. Conestoga Tel & Tel. Co.*, 1999 WL 636664, at *1-*2 (E.D. Pa, Aug. 18, 1999) (holding that a valid subpoena falls within the “except as required by law” exception of § 222(c)(1)).

Magistrate Judge Smith suggests that using the WCPSA to create a Fourth Amendment expectation of privacy in historical cell-site information is consistent with the intent of Congress. *See* Opinion at 33 (“neither should [the judgment of Congress] be ignored”). But given the “strong presumption of constitutionality” of federal statutes challenged on Fourth Amendment grounds, *United States v. Watson*, 423 U.S. 411, 416 (1976), the WCPSA should not be interpreted to undermine the constitutionality of 18 U.S.C. § 2703(d), especially as those two statutes are not in conflict. Moreover, 47 U.S.C. § 222(c)(1) protects not only cell phone location

information; it protects all “individually identifiable customer propriety network information,” which includes dialed phone numbers. Thus, Magistrate Judge Smith’s reasoning suggests that even use of a traditional telephone pen register could violate the Fourth Amendment. This result is inconsistent with *Smith v. Maryland*, and it should be rejected.

B. Compulsory process is subject to a reasonableness standard, not a warrant requirement.

Magistrate Judge Smith’s Opinion is based on the incorrect assumption that if a customer has a reasonable expectation of privacy in historical cell-site records, then a warrant is required to compel their disclosure. This is error. As set forth below, under the basic rules of compulsory process, the United States has a right to every person’s evidence, and the Fourth Amendment does not require a warrant for compulsory process. A 2703(d) order is a form of compulsory process: it is issued by a court on a showing of “specific and articulable facts,” but it otherwise functions as a subpoena. Thus, cases addressing the Fourth Amendment principles applicable to subpoenas also apply to 2703(d) orders.

In this case, cell phone service providers possess information relevant and material to a criminal investigation. The United States therefore has the right to compel its disclosure. “For more than three centuries it has now been recognized as a fundamental maxim that the public . . . has a right to every man’s evidence.” 8 J. Wigmore, *Evidence* § 2192 (McNaughton rev. 1961)); *see also Branzburg v. Hayes*, 408 U.S. 665, 688 (1972) (“‘the public . . . has a right to every man’s evidence,’ except for those persons protected by a constitutional, common-law, or statutory privilege”). As the Supreme Court has explained, “[t]he need to develop all relevant facts in the adversary system is both fundamental and comprehensive. The ends of criminal

justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts.” *United States v. Nixon*, 418 U.S. 683, 709 (1974).

Magistrate Judge Smith’s Opinion treats the compulsory process authority with great skepticism, holding that a warrant will be required for the United States to obtain cell-site records because they “reveal a rich slice of the user’s life, activities, and associations.” Opinion at 34. But the United States’s authority to compel production of existing documents (or the testimony of witnesses) is not limited to information that is vague, inaccurate, or unhelpful. Indeed, compulsory process is regularly used to obtain testimony from close associates, bank records, tax records, credit card records, telephone records, and Internet Protocol address records, all of which may reveal a rich slice of the user’s life. The Opinion’s limited view of the compulsory process authority is contrary to the Supreme Court’s recognition that “[t]o ensure that justice is done, it is imperative to the function of courts that compulsory process be available for the production of evidence needed either by the prosecution or by the defense.” *Nixon*, 418 U.S. at 709. Although there are a few well-established privileges against compulsory process, such as the Fifth Amendment and attorney-client privilege, the Supreme Court has recognized that “exceptions to the demand for every man’s evidence are not lightly created nor expansively construed, for they are in derogation of the search for truth.” *Id.* at 710.

Importantly, the Fourth Amendment does not require a warrant before the United States may compel disclosure of information relevant to a criminal investigation. By its terms, the Fourth Amendment protects people against unreasonable searches and seizures, but it imposes a probable cause requirement only on the issuance of warrants. *See* U.S. Const. amend. IV (“and no Warrants shall issue, but upon probable cause”). The Supreme Court has repeatedly held that

compelled disclosure under the Fourth Amendment is based on a reasonableness standard. For example, in *Wilson v. United States*, 221 U.S. 361, 376 (1911), the Court held that “there is no unreasonable search and seizure when a [subpoena], suitably specific and properly limited in its scope, calls for the production of documents which, as against their lawful owner to whom the writ is directed, the party procuring its issuance is entitled to have produced.” The Court affirmed this rule in *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186, 208 (1946), when it held that “the Fourth [Amendment], if applicable [to a subpoena], at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be ‘particularly described,’ if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant. The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable.”⁴ See also *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 415 (1984); *In re Subpoena Duces Tecum*, 228 F.3d 341, 346-49 (4th Cir. 2000) (discussing the Fourth Amendment’s reasonableness requirement for subpoenas);

⁴The Supreme Court has explained the reason why the Fourth Amendment distinguishes the compulsion of subpoenas from other forms of forcible search and seizure:

‘The latter is abrupt, is effected with force or the threat of it and often in demeaning circumstances, and, in the case of arrest, results in a record involving social stigma. A subpoena is served in the same manner as other legal process; it involves no stigma whatever; if the time for appearance is inconvenient, this can generally be altered; and it remains at all times under the control and supervision of a court.’

United States v. Dionisio, 410 U.S. 1, 10 (1973) (quoting *United States v. Doe*, 457 F.2d 895, 898 (2d Cir. 1972) (Friendly, J.)). Moreover, imposing a probable cause standard on the government’s use of compulsory process ignores a fundamental purpose for compelled disclosure: to determine whether probable cause exists. As the Supreme Court has explained in the context of subpoenas, “the Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists.” *United States v. R Enterprises, Inc.*, 498 U.S. 292, 297 (1991).

Newfield v. Ryan, 91 F.2d 700, 703-05 (5th Cir. 1937) (upholding subpoena to a telegraph company for certain telegrams in its possession that had been sent or received by the targets of an investigation).

Magistrate Judge Smith's Opinion implicitly assumes that if a customer has a reasonable expectation of privacy in historical cell-site information, then a warrant is required to compel disclosure of such records. However, the Fourth Amendment imposes a reasonableness requirement on compulsory process regardless of the existence of a reasonable expectation of privacy. *See, e.g., United States v. Palmer*, 536 F.2d 1278, 1281-82 (9th Cir. 1976) ("We do not explore the issue of a reasonable expectation of privacy, however, because the use of a properly limited subpoena does not constitute an unreasonable search and seizure under the Fourth Amendment."). Indeed, nearly every document subject to compulsory process is likely to be stored in a home, office, filing cabinet, or some other closed container in which there may be a reasonable expectation of privacy. Importantly, the issue before the Supreme Court in *Miller* was not whether a warrant was required to obtain the defendant's bank records. Instead, the issue in *Miller* was whether the defendant had a sufficient Fourth Amendment interest to challenge the use of bank records obtained pursuant to a *defective* subpoena, not whether a warrant would be required to obtain bank records. *See Miller*, 425 U.S. at 438-39.

To be clear, the government's authority to compel an entity to disclose an item or information via 2703(d) order is limited to items or information over which the entity has joint access or control for most purposes. This rule is consistent with the common authority doctrine of *United States v. Matlock*, 415 U.S. 164, 172 n.7 (1974), and also with the rule that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed

by him to Government authorities.” *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (quoting *Miller*, 425 U.S. at 443 (citing *Hoffa v. United States*, 385 U.S. 293, 302 (1966))). But a cell-phone provider’s authority to access its own historical cell-site records is not limited; it has the same authority to access them as it does its other call detail records. Thus, a warrant is not required for the government to compel a provider to disclose historical cell-site records.

- C. Even under the standards applicable to surreptitiously installed tracking devices, the Fourth Amendment does not bar compelled disclosure of historical cell-site records.

The Opinion further errs in holding that warrantless disclosure of cell-site records violates the Fourth Amendment under the tracking device cases *United States v. Karo*, 468 U.S. 705 (1984), and *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010). See Opinion at 35. As business records in the possession of a third party, cell-site records should not be judged under Fourth Amendment standards applicable to tracking devices surreptitiously installed by the government. For example, a pen register on a landline telephone will typically disclose that a phone call was made from a private home at a particular time. A pen register is permissible under *Smith v. Maryland*, and it should thus not be judged under the tracking device standards of *Karo*.

But even measured against the constitutional standards articulated by the Supreme Court in *Karo* regarding surreptitiously installed tracking devices, the United States would not violate the Fourth Amendment when it obtains historical cell-site information without a warrant. The Supreme Court has made clear that mere use of a tracking device, even when surreptitiously placed by the government, does not implicate Fourth Amendment privacy concerns. See *United States v. Knotts*, 460 U.S. 276, 282 (1983) (police monitoring of beeper signals along public

roads did not invade any legitimate expectation of privacy). To be of constitutional concern, a surreptitiously installed tracking device must reveal facts about the interior of a constitutionally protected space. *See United States v. Karo*, 468 U.S. at 715 (distinguishing *Knotts* and holding that police monitoring of a beeper that disclosed information about the interior of a private residence, not open to visual surveillance, required a warrant).

At issue in *Karo* was not whether persons or objects in private spaces enjoy generalized and undifferentiated Fourth Amendment protection. Rather, as the Court explains at the outset, the exact question is “whether monitoring of a beeper falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance.” *Id.* at 707. In that case, agents had installed a radio transmitter in a can of ether expected to be used in processing cocaine. Without first obtaining a warrant, the agents monitored the signal from the beeper as it moved through a series of residences and multi-unit storage facilities. *See id.* at 708-09. Where the tracking system enabled the government to locate the can of ether in particular residences, the Supreme Court found that the Fourth Amendment had been infringed. *See id.* at 715 (“The beeper tells the agent that a particular article is actually located at a particular time in the private residence [L]ater monitoring . . . establishes that the article remains on the premises.”).

Conversely, the Court found no Fourth Amendment violation where the beeper disclosed only the general location of the ether. In particular, “the beeper equipment was not sensitive enough to allow agents to learn precisely which locker [in the first storage facility] the ether was in.” *Id.* at 708. Instead, the agents learned the can’s precise location inside a specific locker only after subpoenaing the storage company for rental records; tracking the beeper to a specific row of

lockers; and then using their sense of smell to detect the ether. *See id.*

As to these two episodes, the Supreme Court held emphatically that no Fourth Amendment violation occurred:

[T]he beeper informed the agents only that the ether was somewhere in the warehouse; it did not identify the specific locker in which the ether was located. Monitoring the beeper revealed nothing about the contents of the locker that Horton and Harley had rented and hence was not a search of that locker.

Id. at 720. In sum, the test under *Karo* is not simply whether a tracked object is inside a private, constitutionally protected pocket, purse, or home. (The can of ether was at the relevant times unquestionably in each of the two lockers, both of which enjoyed a reasonable expectation of privacy. *See id.* at 720 n.6.) Rather, *Karo* holds that government use of a tracking device violates the Fourth Amendment only where the monitoring actually reveals the *particular* private location in which the tracked object may be found.

Based on this standard from *Karo*, cell-site records of MetroPCS and T-Mobile are not precise enough to implicate the Fourth Amendment. The MetroPCS affidavit demonstrates that its cell-site records can only reveal a telephone's location to within one to two miles on average and to within at least a hundred yards in densely populated urban areas. The United States believes that testimony from T-Mobile would demonstrate similar accuracy in its historical cell-site records. As a result, such information cannot reveal whether a telephone is within a constitutionally protected private space (such as a residence) and therefore does not implicate any Fourth Amendment-protected privacy interests. *See United States v. Ortega-Estrada*, 2008 WL 4716949, at *13 (N.D. Ga. Oct. 22, 2008) (finding that even GPS information accurate to within 32 meters "revealed only a general area where the suspect was at a particular time, and thus, did

not invade a place where he might have an expectation of privacy”).

The Opinion further errs in relying on *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), to support its holding that warrantless disclosure of cell-site records violate the Fourth Amendment. *Maynard* held that agents violated the Fourth Amendment after they covertly installed a GPS device on a car when they tracked the car’s movements for 28 days. *Maynard* promulgated a new “intimate picture” or “mosaic” theory of the Fourth Amendment, under which “[t]he whole of one’s movements over the course of a month is not constructively exposed to the public,” even though one’s individual movements are exposed to the public. *Id.* at 561-62. *Maynard*’s holding is inconsistent with the basic rule that “[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.” *Katz v. United States*, 389 U.S. 347, 351 (1967). *Maynard* is also inconsistent with the Court’s holding in *Smith v. Maryland*: a reasonable person would not expect the phone company to closely monitor the network of people he calls in an attempt to draw inferences about the scope of his conduct and connections. As one district court recently explained in rejecting *Maynard*, *Maynard*’s rationale “is essentially that the whole of one’s movements during the course of surveillance is not actually exposed to the public because the likelihood that anyone will observe all those movements is essentially nil. . . . The proper inquiry, however, is not what a random stranger would actually or likely do, but rather what he feasibly could.” *United States v. Sparks*, ___ F. Supp. 2d ___, 2010 WL 4595522, at *6 (D. Mass. Nov. 10, 2010) (citing *Smith v. Maryland*).

Furthermore, *Maynard* is “vague and unworkable.” *Sparks*, 2010 WL 4595522 at *8. Under *Maynard*, “[i]t is unclear when surveillance becomes so prolonged as to have crossed the threshold and created this allegedly intrusive mosaic. What’s more, conduct that is initially

constitutionally sound could later be deemed impermissible if it becomes part of the aggregate.”

Id. This “retroactive unconstitutionality” is not a feature of any other Fourth Amendment doctrine. The *Maynard* decision conflicts with the opinions of three other courts of appeals on the use of tracking devices, and it should be rejected. *See United States v. Marquez*, 605 F.3d 604, 609-10 (8th Cir. 2010); *United States v. Pineda-Moreno*, 591 F.3d 1212, 1216-17 (9th Cir. 2010); *United States v. Garcia*, 474 F.3d 994, 997-98 (7th Cir. 2007).

Any reliance on *Maynard* is mistaken, but extending the mosaic theory of *Maynard* to historical cell-site information goes far beyond even *Maynard*’s reasoning. First, *Maynard*’s mosaic rationale is inconsistent both with business records cases such as *Miller* and *Smith v. Maryland* and with more recent cases applying these principles to the Internet, such as *United States v. Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2008) (holding that pen register/trap and trace device for email addresses and IP addresses did not violate Fourth Amendment). Such business records often supply an “intimate picture” of a user’s life, but they are unprotected by the Fourth Amendment. Expansion of *Maynard* to the realm of compulsory process would replace the rule that the United States is entitled to every person’s evidence with a rule that the United States is entitled to every person’s evidence, unless the person knows a lot about the target of the investigation. Second, *Maynard* involves a tracking device covertly installed by the government that continuously monitors movements at all times, but historical cell-site records involve only records of a user’s location at the beginning and end of phone calls. Third, historical cell-site records are much less precise than the GPS information of *Maynard*. Fourth, *Maynard* does not preclude all warrantless tracking; instead, warrantless tracking by the government is evaluated after the fact via a motion to suppress or other appropriate litigation. In contrast, the Opinion

precludes the government from obtaining any historical cell-site information using a 2703(d) order. Thus, Magistrate Judge Smith erred in applying *Maynard* to historical cell-site records.

Conclusion and Relief Sought

For these reasons, the United States respectfully submits that this Court should reverse Magistrate Judge Smith's Opinion and grant the applications for historical cell-site information. The United States submits that this Court should reject the Opinion's "findings of fact" as subject to reasonable dispute under Rule 201, and it should reverse the Opinion because a customer has no privacy interest in business records held by a cell phone provider and because the Fourth Amendment sets a reasonableness standard for compulsory process. In addition, this Court may reverse the Opinion because the historical cell-site records of MetroPCS and T-Mobile are insufficiently precise to reveal whether a telephone is within a constitutionally protected private space. If this Court wishes to make findings of fact regarding the precision of T-Mobile's historical cell-site records, it may be helpful for this Court to obtain testimony from T-Mobile. However, such testimony is not essential to resolving this case.

Respectfully submitted,

JOSE ANGEL MORENO
UNITED STATES ATTORNEY

By: Eric D. Smith /s/
Eric D. Smith
Assistant United States Attorney

Nathan Judish
Senior Counsel, Computer Crime and
Intellectual Property Section
U.S. Department of Justice